

IN THE ABSTRACT

Please amend the Abstract as follows:

-- The present invention provides a A symmetric-key cryptographic technique capable of realizing both high-speed cryptographic processing having a high degree of parallelism, and alteration detection. The present invention includes ~~performs the~~ steps of: dividing plaintext composed of redundancy data and a message to generate a plurality of plaintext blocks each having a predetermined length; generating a random number sequence based on a secret key; generating a random number block corresponding to one of said plurality of the plaintext blocks from said the random number sequence; outputting a feedback value obtained as a result of operation on said the one of the plurality of plaintext blocks and said the random number block, said the feedback value being fed back ~~to~~ for using in the operation on another one of the plurality of plaintext blocks; and performing an encryption operation using said the one of the plurality of plaintext blocks, said random number block, and a feedback value obtained as a result of operation on still another one of the plurality of plaintext blocks to produce a ciphertext block. --